



**UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE FINANÇAS E CONTABILIDADE
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS**

DANYEL TARGINO PEREIRA

**CIBERSEGURANÇA: A PERCEPÇÃO DOS USUÁRIOS DE *INTERNET BANKING*
DO CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS DE UMA
UNIVERSIDADE PÚBLICA FEDERAL NA CIDADE DE JOÃO PESSOA**

**JOÃO PESSOA
2020**

DANYEL TARGINO PEREIRA

**CIBERSEGURANÇA: A PERCEPÇÃO DOS USUÁRIOS DE *INTERNET BANKING*
DO CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS DE UMA
UNIVERSIDADE PÚBLICA FEDERAL NA CIDADE DE JOÃO PESSOA**

Monografia apresentada ao Curso de Ciências Contábeis, do Centro de Ciências Sociais Aplicadas, da Universidade Federal da Paraíba, como requisito parcial para a obtenção do grau de Bacharel em Ciências Contábeis.

Orientador: Prof. Dr. Tiago Henrique de Souza Echternacht

**JOÃO PESSOA
2020**

P436c Pereira, Danyel Targino.

CIBERSEGURANÇA: A PERCEPÇÃO DOS USUÁRIOS DE INTERNET
BANKING DO CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS DE
UMA UNIVERSIDADE PÚBLICA FEDERAL NA CIDADE DE JOÃO
PESSOA / Danyel Targino Pereira. - João Pessoa, 2020.
40 f.

Monografia (Graduação) - UFPB/CCSA.

1. CIBERSEGURANÇA. 2. INTERNET BANKING. 3. SISTEMA DE
INFORMAÇÃO. I. Título

UFPB/BC

DANYEL TARGINO PEREIRA

**CIBERSEGURANÇA: A PERCEPÇÃO DOS USUÁRIOS DE *INTERNET BANKING*
DO CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS DE UMA
UNIVERSIDADE PÚBLICA FEDERAL NA CIDADE DE JOÃO PESSOA**

Esta monografia foi julgada adequada para a obtenção do grau de Bacharel em Ciências Contábeis, e aprovada em sua forma final pela Banca Examinadora designada pela Coordenação do TCC em Ciências Contábeis da Universidade Federal da Paraíba.

BANCA EXAMINADORA

Presidente: Prof. Dr. Tiago Henrique de Souza Echternacht
Instituição: UFPB

Membro: Prof. Dr. Epitácio Ezequiel de Medeiros
Instituição: UFPB

Membro: Prof. Me. Marcelo Pinheiro de Lucena
Instituição: UFPB

João Pessoa, 31 de março de 2020.

Dedico este Trabalho aos meus pais, Admilson Pereira e M^a de Lourdes Targino Pereira, e ao meu irmão Dyego, por todo o esforço, dedicação, amor, respeito e apoio em cada momento de minha vida.

AGRADECIMENTOS

Dou graças a Deus pelo dom da vida, e agradeço a Ele por ter me mostrado todos os caminhos que eu teria que trilhar para estar aqui hoje, concluindo meu curso, por estar sempre ao meu lado segurando minha mão e levantando todas às vezes a minha cabeça nos momentos mais difíceis durante a caminhada da vida. Agradeço por todas as dificuldades enfrentadas e superadas que tornam este momento possível.

Aos meus pais, Admilson Pereira e M^a de Lourdes Targino Pereira pela criação, educação, dedicação, pelo carinho e o amor sem medidas, não só a mim, mas também ao meu irmão, Dyego. Essa vitória é tão minha quanto de vocês, que me possibilitaram chegar até aqui.

Agradeço a minha avó, Sebastiana “Vó Mocinha” Freire (*in memoriam*). Por todos os ensinamentos e pelo o seu carinho imensurável, por todo amor que me proporcionou e por ter me ensinado grandes lições que a vida pode nos ensinar. *“Deus escolheu o dia mais certo para que ela fosse morar com Ele, que para os cristãos representava naquele ano então, o Sábado de Aleluia, que é o dia em que se acende o Círio Pascal [uma grande vela] que simboliza a Luz de Cristo, que ilumina o mundo. Que era isso que ela representou em vida... Luz. A sua bênção minha vó!”*

Aos amigos Jotan Martins, Tialisson Lima, Ítalo Miranda, José Danilo Lima, que me acompanharam em toda essa jornada acadêmica e que se mostraram presentes em minha conquista, proporcionando sempre apoio e palavras de determinação. A amizade não é feita só de presença, mas de atitudes que não nos deixam esquecer o real valor das pessoas e a importância delas em nossas vidas.

Agradecer também a minha amiga, companheira, e namorada, Jokasta Nascimento que sem o apoio em todos os sentidos não teria conseguido concluir esse trabalho.

A todos os professores que colaboraram para a formação do conhecimento. Em especial aos Professores Wenner Lucena, Azamor Cirne, Jaimar Medeiros, Marcelo Pinheiro, Manaíra Abrantes, Edmery Tavares, pelo prazer e privilégio de ter convivido com excepcionais mestres e acima de tudo, grandes pessoas.

Ao Dr. Tiago Echternacht, meu orientador, pela disposição, dedicação e paciência ofertada durante a realização deste trabalho.

RESUMO

Este trabalho tem como objetivo avaliar a percepção dos alunos de graduação do curso de Ciências Contábeis da Universidade Federal da Paraíba (UFPB) acerca da segurança dos dados fornecidos por eles ao banco de dados da *internet banking* das instituições financeiras que utilizam, sejam estas através de computadores, notebooks, tablets e/ou smartphones. As instituições financeiras e os bancos promovem frequentes alterações em seu modelo de negócios, através de inovações em seus produtos, serviços, canais de distribuição, sistemas de informação e atendimento ao cliente. Essas inovações visam a busca da fidelização do cliente e resultados financeiros positivos e crescentes. A metodologia utilizada foi através de revisão bibliográfica e estudo de casos realizados em trabalhos já publicados, a coleta de dados foi realizada através de um questionário e estes foram analisados de forma quantitativa e descritiva. Como forma de atingir esses objetivos, foi feito uso de métodos estatísticos, com a utilização de análise de gráficos.

Palavras-chave: *Internet banking*. Cibersegurança. Sistema de informação.

ABSTRACT

This work aims to evaluate the perception of undergraduate students in the Accounting Sciences course at the Federal University of Paraíba (UFPB) about the security of data provided by them to the internet banking database of the financial institutions they use, be it through computers, notebooks, tablets and/or smartphones. Financial institutions and banks promote frequent changes in their business model through innovations in their products, services, distribution channels, information systems and customer service. These innovations are aimed at seeking customer loyalty and positive and growing financial results. The methodology used was carried out through bibliographic review and case studies carried out in already published works, data collection was done through a questionnaire and these were analyzed in a quantitative and descriptive manner. In order to achieve these objectives, statistical methods were used, with the use of graph analysis.

Keywords: Internet banking. Cybersecurity. System of information.

LISTA DE GRÁFICOS

Gráfico 1 – Gênero.....	20
Gráfico 2 – Faixa etária	21
Gráfico 3 – Adeptos das transações bancárias	22
Gráfico 4 – Meios digitais utilizados nas operações bancárias	23
Gráfico 5 – Verificar operações e transações bancárias	24
Gráfico 6 – Realização de transferências.....	24
Gráfico 7 – Realização de depósitos bancários	25
Gráfico 8 – Realização de saques bancários	26
Gráfico 9 – Realização de pagamentos	26
Gráfico 10 – Conhecimentos de incidentes digitais.....	28
Gráfico 11 – Conhecimentos de medidas contra incidentes digitais	29
Gráfico 12 – Conhecimentos de ciberataque	29
Gráfico 13 – Conhecimentos dos riscos de incidentes digitais.....	30
Gráfico 14 – Conhecimentos de ciberataque nos últimos anos	31
Gráfico 15 – Conhecimentos de informações sobre cibercrimes	32

LISTA DE ABREVIATURAS E SIGLAS

CFC	Conselho Federal de Contabilidade
FEBRABAN	Federação Brasileira de Bancos
TI	Tecnologia da Informação
UFPB	Universidade Federal da Paraíba

SUMÁRIO

1	INTRODUÇÃO	10
1.1	PROBLEMA DA PESQUISA	11
1.2	OBJETIVOS.....	11
1.2.1	Objetivos Geral	11
1.2.2	Objetivos Específicos.....	12
1.3	JUSTIFICATIVA.....	12
2	REVISÃO DA LITERATURA.....	13
2.1	INTERNET BANKING NO BRASIL	13
2.2	CIBERSEGURANÇA	15
2.3	SEGURANÇA NACIONAL	16
3	METODOLOGIA.....	18
3.1	TIPOLOGIA DO ESTUDO.....	18
3.2	POPULAÇÃO E AMOSTRA.....	18
3.3	PROCEDIMENTOS DE COLETA E ANÁLISE DOS DADOS	19
4	APRESENTAÇÃO E ANÁLISE DOS RESULTADOS	20
4.1	PERFIL DOS PARTICIPANTES	20
4.2	USUÁRIOS DE OPERAÇÕES BANCÁRIAS POR MEIO DIGITAL	21
4.3	CONHECIMENTO DE CIBERCRIMES	27
5	CONSIDERAÇÕES FINAIS	33
	REFERÊNCIAS.....	34
	APÊNDICE A – QUESTIONÁRIO.....	36

1 INTRODUÇÃO

O rápido avanço tecnológico trouxe para a sociedade necessidades de adequar-se à nova realidade. A velocidade com que as informações são disseminadas exigem que todos os indivíduos, seja o que usa a tecnologia para atividades simples do dia-a-dia ou até a empresa que utiliza a tecnologia para aumentar o alcance aos seus clientes, estejam integrados e incorporados a esta evolução.

Apesar da imensurável quantidade de vantagens que a tecnologia proporciona existe uma questão que está intrínseca à veiculação de tais informações, que é a segurança, para este fim. Utiliza-se o termo cibersegurança, esta pode ser definida como “a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. Também é chamada de segurança de tecnologia da informação ou segurança de informações eletrônicas” (KASPERSKY, 2019).

Em um contexto cada vez mais voltado para a acessibilidade da informação, as instituições financeiras na prestação dos seus serviços, na obtenção e disponibilização de informações e na interação com seus clientes através da internet visam a qualidade desta troca de informações.

Jun e Cai (2001, p. 276) atestam que inúmeros estudos foram realizados identificando os aspectos chaves na avaliação da qualidade do serviço para bancos tradicionais, onde a interação pessoal entre os consumidores e os funcionários dos bancos é o canal básico de comunicação e entrega de serviço.

Para Strong, Lee e Wang (1997), a informação deve ser orientada como um produto e, conseqüentemente, a qualidade da informação deve ser avaliada de acordo com sua adequação para os fins aos quais ela se destina.

O presente trabalho se propõe a avaliar a percepção dos usuários de uma universidade pública federal, quanto à qualidade da informação de sistemas baseados na internet, especificamente os sistemas desenvolvidos por instituições financeiras para apoio a esses seus clientes em suas transações bancárias (pagamentos, transferências, emissão de extratos, etc.), aqui denominado de *internet banking* e também a identificar o acesso dos usuários a suas instituições financeiras e bancárias, a sua percepção acerca da segurança na troca de informações que envolve estes recursos, e a relevância da implantação e implementação de segurança da informação por meio do seu canal, *internet banking*.

1.1 PROBLEMA DA PESQUISA

Um estudo feito desde 2015, com últimos resultados em 2017, feito pela empresa de auditoria *Binder Dijker Otte* (BDO), uma das cinco maiores empresas de contabilidade do mundo, denominado “Relatório de fatores de risco do varejo”, para os 100 maiores varejistas americanos, elencam os principais riscos para estas organizações, em primeiro lugar com as condições econômicas do país, estão preocupações de privacidade relacionados à violação de segurança, e com implementação e manutenção de Sistemas de Tecnologia da Informação (TI), também estavam entre os 10 primeiros maiores riscos listados. (BDO, 2017).

O último Relatório Global de Fraude e Risco 2019/2020, divulgado pela Kroll (2019), uma divisão da Duff e Phelps, e líder global em soluções de mitigação de riscos, investigações, conformidade, resiliência cibernética, segurança e resposta a incidentes, revela que as empresas globais enfrentam agora um cenário de risco ainda mais amplo, à medida que as organizações buscam enfrentar ameaças digitais emergentes e lidar com questões complexas de reputação e regulamentação. O risco mais comum, sofrido por 39% das empresas globais, são vazamentos de informações internas, destacando a crescente ameaça interna à propriedade intelectual, segredos comerciais e outras informações confidenciais.

Nessa situação e a partir das considerações teóricas, surge o seguinte questionamento: **qual a percepção dos usuários do serviço de *Internet banking* acerca da qualidade da segurança ofertada pelas instituições financeiras, em uma universidade pública federal na cidade de João Pessoa?**

1.2 OBJETIVOS

A pesquisa se apresenta estruturada em um objetivo geral e três objetivos específicos, conforme observado a seguir.

1.2.1 Objetivos Geral

Este trabalho tem como objetivo geral avaliar a percepção dos alunos de graduação do curso de Ciências Contábeis da Universidade Federal da Paraíba

acerca da segurança dos dados fornecidos por eles ao banco de dados da *internet banking* das instituições financeiras que utilizam.

1.2.2 Objetivos Específicos

- a) Verificar o conhecimento dos incidentes digitais por meio do uso de *internet banking*;
- b) Verificar o conhecimento dos tipos de medidas contra os incidentes digitais;
- c) Verificar o conhecimento dos discentes sobre cibersegurança.

1.3 JUSTIFICATIVA

A empresa de investigação americana, Kroll (2019), divulgou um estudo denominado, *Global Fraud and Risk Report 2019/20 11TH ANNUAL EDITION*, informações preocupantes a respeito de fraudes empresariais no Brasil. Segundo o levantamento, 74% das organizações teriam sofrido ao menos um episódio de fraude nos 12 meses anteriores à pesquisa.

Os avanços aconteceram e continuarão a sobrevir ocupando cada vez mais espaço e exigindo mais contato com este. Os serviços de *internet banking* acompanham a necessidade de agilidade para solucionar tarefas que antes levavam horas para serem concluídas, o que antes demandava muito tempo para enfrentar filas e deslocamento, hoje está ao alcance das mãos com apenas um toque e em qualquer lugar que esteja bastando ter acesso a internet. Visualizar extratos, realizar movimentações financeiras, pagamentos, transações etc. No entanto à margem desta facilidade está um montante de informações sigilosas e que necessitam de proteção.

Neste trabalho será possível avaliar através de pesquisa com usuários de *internet banking* a segurança dos dados que circulam na internet, também chamada de cibersegurança.

2 REVISÃO DA LITERATURA

O objetivo deste tópico foi estabelecer a relação teórica dos principais temas da pesquisa. Dessa maneira, procura-se contemplar os seguintes assuntos: transformação digital, tecnologia da informação e documentos digitais.

2.1 *INTERNET BANKING* NO BRASIL

O *internet banking* é, em linhas gerais, mais um dos serviços ofertados pelos bancos, através da internet, associando à demanda dos clientes por maior conveniência e interesse dos bancos por economia, precisão e automação.

De acordo com Mattar e Takaoka (2005, p. 24), este pode ser melhor definido como sendo “uma solução de informática que permite o acesso a serviços bancários no local e no momento que o cliente assim o desejar, o que torna dispensável o comparecimento à agência bancária”.

O *internet banking* hoje é um dos serviços mais utilizados pelos clientes, apesar de no início ser considerado apenas mais um canal para a distribuição de serviços bancários, mas que passou por constantes evoluções tanto dos bancos quanto dos seus clientes.

Algumas outras estratégias foram utilizadas antes da adoção propriamente dita de um sistema baseado na internet, a exemplo do *home banking*, considerado predecessor do *internet banking*. Para Estrada (2005, p. 140) estes “termos técnicos não se confundem, pois, o *internet banking* precisa de acesso à rede bancária e que dispensa a prévia instalação de sistemas proprietários dos bancos nos computadores de seus clientes”.

Hoje poucas são as visitas regulares aos caixas que têm sido substituídas pelo *internet banking*. E quem utiliza desta ferramenta hoje em dia nem imagina como foram os primeiros passos desta tecnologia. Utilizado pela primeira vez, nos Estados Unidos, em 9 de outubro de 1980. No início eram bem diferentes de como a conhecemos hoje, tanto a evolução e a prática da *internet banking*. Onde para o cliente poder acessar a sua conta e realizar uma operação bancária era necessário realizá-la por meio do telefone fixo.

A preferência desta ferramenta se justifica pela comodidade e conveniência de poder utilizar o serviço a qualquer hora e estar em qualquer lugar para fazer quaisquer

movimentações financeiras (pagamentos de contas, transferências de valores, contratar empréstimos e consultar extratos, etc.).

O serviço de *internet banking* é criado e ofertado ao usuário como um serviço protegido. A segurança na transmissão de dados se dá de forma criptografada¹, o que faz com que seus usuários fiquem menos vulneráveis a riscos. Alternativas individualizadas, aumentam a segurança no serviço, pois este meio de acesso é intransferível e inviolável, todavia existe a possibilidade de erros no sistema, uma vez que o serviço é alimentado por um servidor².

No ano de 2017, segundo a Federação Brasileira de Bancos (Febraban) divulgou que o celular era o canal preferido dos brasileiros para fazer transações bancárias, o chamado *mobile banking*, com 34% das movimentações financeiras. Em segundo lugar estava o *internet banking*, com 23% do total. Isso significa que, mais da metade das transações bancárias, no Brasil, têm sido resolvidas pela internet.

O número de contas que usam *mobile banking* saltou de 57 milhões em 2017 para 70 milhões em 2018, enquanto os usuários que realizam pelo menos 80% das transações por esse canal, chamados *heavy users*, passaram de 16,3 milhões em 2017 para 26,8 milhões em 2018.

De acordo com essa mesma pesquisa afirma-se ainda que o setor bancário é o que mais investe em tecnologia dentre todas as indústrias mundialmente. Onde apenas em 2018, R\$19,6 bilhões foram aplicados em tecnologia pelas instituições financeiras, com o objetivo de melhor atender às necessidades dos clientes em um mundo de rápida transformação tecnológica; um crescimento de 3% em relação a 2017. Houve um aumento nas despesas com tecnologia, que subiram de R\$ 13,2 bilhões para R\$ 13,9 bilhões. Os investimentos, por sua vez, mantiveram-se no mesmo patamar, indo de R\$ 5,8 bilhões para R\$ 5,7 bilhões – reflexo do esforço dos bancos em acompanhar a evolução da tecnologia, de forma eficiente, para oferecer serviços de ponta aos seus clientes.

¹ Camuflagem pelo qual a informação passa, onde apenas o emissor e o receptor têm acesso.

² É um computador equipado com um ou mais processadores, capaz de executar um conjunto específico de programas ou protocolos para fornecer serviços para outras máquinas ou clientes.

2.2 CIBERSEGURANÇA

O mundo digital que faz parte da vida da maioria das pessoas na atualidade tem se modificado com a finalidade de aperfeiçoar e criar novas possibilidades para a transmissão e arquivamento de informações. O termo ciberespaço foi criado em 1984 por William Gibson, citado em seu livro *Neuromancer* (1984), e é definido como um espaço existente no mundo da comunicação. Neste meio é possível se relacionar e comunicar-se com os indivíduos. Essas relações são possíveis para pessoas e/ou instituições financeiras que necessitam interligar-se, não só entre si, mas também interligar-se a uma rede de informações que pressupõem máquinas e documentos.

O ciberespaço é o meio que o governo, as pessoas e as empresas utilizam para transmitir informações e armazenar dados. Todos estes possuem importância, sejam estes dados pessoais a exemplo de informações de redes sociais, como os dados do governo. O vazamento de tais informações causaria um verdadeiro caos e é com a finalidade de reduzir tais riscos e ameaças que existe a cibersegurança.

Esta prática é definida como sendo a que protege computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. Os atos ilícitos neste meio são tão aprimorados quanto os que são criados para proteger as informações dos usuários.

Segundo Antunes, Rodrigues (2018),

O aumento crescente e exponencial da Internet, quer ao nível geográfico, quer no número de utilizadores e serviços disponibilizados, lançou vários desafios e potencializou o aparecimento de um vasto conjunto de ameaças no ciberespaço. Se, por um lado, a implementação de medidas reativas de segurança na internet conduz tendencialmente à diminuição de ameaças, por outro lado, a prevenção e a formação contínua dos utilizadores podem revelar-se um forte aliado na implementação de medidas proativas e que evitem a execução de tais ameaças.

Ao redor do mundo organizações terroristas utilizam deste canal para conquistar seus objetivos. A isso se deve o alto investimento de capital em proteção do ciberespaço. “As organizações terroristas e os seus apoiantes, por exemplo, usam frequentemente a Internet para tarefas como recolhimento de informações, recrutamento de novos membros, financiamento entre outras operações” (ANTUNES; RODRIGUES, 2018).

Os desafios na cibersegurança são inúmeros, tendo em vista o crescente avanço tecnológico e das novas possibilidades criadas em rede. O investimento faz-se necessário a fim de conseguir proteger informações que são vitais para o bom funcionamento das instituições governamentais e pessoais.

2.3 SEGURANÇA NACIONAL

Quando falamos em segurança estamos nos referindo às diversas vertentes. Podemos citar segurança com alimentos, nuclear, pública, econômica, entre tantas outras.

As movimentações financeiras estão incluídas nas preocupações de uma nação, bem como, a segurança da tecnologia, seja a nível nacional ou mundial. As circulações dos dados dos cidadãos requerem atenção e proteção uma vez que podem afetar diretamente a economia do país. No mundo, os investimentos em segurança têm sido tratados com mais veemência.

Os Estados Unidos são pioneiros no desenvolvimento da tecnologia da informação e por assim ser recebem investimentos estrangeiros para este fim. No tocante a segurança da informação todos são beneficiados por esses investimentos, uma vez que é possível normatizar as leis de segurança nacional de acordo com cada regulamentação interna de cada país.

De acordo com Kroll (2019),

Dado o recente aumento geral das tensões geopolíticas e uma maior sensibilidade para proteger a tecnologia de um país e os dados de seus cidadãos, é provável que muitos efeitos colaterais emanem da ampliação das preocupações de segurança nacional. Um exemplo vívido do papel ampliado das preocupações de segurança nacional na política comercial envolve o *Committee on Foreign Investment in the United States* (CFIUS), que avalia os investimentos estrangeiros nos Estados Unidos de uma perspectiva de segurança nacional.

Essas organizações esperam que essas normas tenham cada vez mais um papel preponderante no comércio mundial, e que essas normas entrem em harmonia no combate à lavagem de dinheiro e anticorrupção entre poderes, ilustrando muito bem como essas adesões podem evoluir. Segundo dados da pesquisa, *Global Fraud and Risk Report 2019/2020* (Relatório Global de Fraude e Risco 2019/2020), mais do

que nunca, as empresas precisam considerar as preocupações de segurança nacional como um risco comercial (KROLL, 2019).

Pois cada movimento tem que ser pensado e dado com maior presteza nessas questões de segurança nacional com o mesmo enfoque que é dado aos conteúdos contra as manipulações de valores.

No que diz respeito a segurança da informação o Brasil apresenta motivos importantes para justificar o investimento nessa área. O combate a corrupção tem sido pauta recorrente, sendo esta uma causa importante a ser discutida e combatida uma vez que subornos acontecem com facilidade no país a exemplo da lavagem de dinheiro. As informações são roubadas e/ou manipuladas com frequência e este motivo segundo o Relatório Global de Fraude e Risco 2019/2020, é a principal prioridade de risco para os brasileiros seguido de vazamento de informações internas.

Segundo Kroll (2019),

Os entrevistados no Brasil são mais propensos do que os participantes de qualquer outro país da pesquisa a reportar vazamentos de informações internas, que geralmente ocorrem através de redes de computadores (55% vs. 39% no mundo); eles também nomeiam o roubo de dados como sua principal prioridade de risco (84% vs. 76% globalmente).

3 METODOLOGIA

Nesta seção, serão descritas as tipologias utilizadas para realização da pesquisa, a coleta, a análise e a sistematização dos dados, população e amostra, bem como os procedimentos metodológicos para aplicação do levantamento.

3.1 TIPOLOGIA DO ESTUDO

Para a realização desse estudo, foi utilizada a pesquisa com tipologia descritiva. Segundo Selltiz, Wrightsman e Cook (1987), nos estudos descritivos uma consideração fundamental é a exatidão; portanto, é necessário um planejamento que amplie a precisão da prova obtida. Este tipo de estudo tem como objetivo verificar a frequência com que algo ocorre e descobrir ou verificar a ligação entre determinadas variáveis. São utilizadas técnicas padronizadas para a coleta de dados, neste caso, foi utilizada a aplicação de questionários.

Quanto aos procedimentos, a pesquisa caracteriza-se como levantamento, também conhecida como *survey*, que, conforme Gil (2002, p. 50), “caracterizam-se pela interrogação direta das pessoas cujo comportamento se deseja conhecer procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado”, com isso, se faz uma análise quantitativa, para alcançar as conclusões correspondentes aos fatos pesquisados.

Quanto à abordagem do problema, a pesquisa se enquadra como quantitativa, que de acordo com Collins e Hussey (2005), a pesquisa quantitativa se caracteriza por utilizar métodos estatísticos na coleta e tratamento dos dados, fornecendo informações que podem ser generalizáveis.

3.2 POPULAÇÃO E AMOSTRA

O universo investigado da pesquisa foram os alunos matriculados regularmente ativos no curso de Ciências Contábeis na UFPB no Campus I, que estavam entre o 1º e 8º período, no caso de alunos do turno da manhã, e do 1º ao 10º período, para os alunos do turno da noite.

Segundo a coordenação do curso, existem 811 alunos ativos, segundo site do curso na internet. Deste total de alunos, foi obtida a amostra de 93 discentes para a

pesquisa, sendo assim, a pesquisa foi feita por acessibilidade e conveniência, onde a seleção dos entrevistados depende da sua disponibilidade para responder o questionário, conforme Sampieri, Collado e Lúcio (2013).

3.3 PROCEDIMENTOS DE COLETA E ANÁLISE DOS DADOS

Para analisar a percepção dos usuários da UFPB quanto à qualidade e segurança do serviço de *internet banking*, a pesquisa foi realizada com aplicação de questionário, elaborado com a finalidade de mensurar as características qualitativas desse serviço.

O questionário aplicado (APÊNDICE A) consistia em questões diretas, divididas em três etapas. A primeira etapa consistia em traçar, brevemente, o perfil dos respondentes no que tange características de gênero e faixa etária. A segunda etapa focava no perfil do usuário de operações por meio digital, como tipo de transações bancárias, os meios digitais utilizados nas transações bancárias, quais canais utilizados nas operações feitas recentes, como realiza transferência de recursos, como faz depósitos bancários, quais meios para sacar dinheiro, quais meios utilizavam para pagamento. Já a terceira e última parte do questionário, questionava os discentes quanto aos conhecimentos de cibersegurança, a fim de investigar se conheciam aspectos de incidentes digitais, como fraudes de *phishing*, ataques de negação, engenharia social, se tinham conhecimento também de medidas de segurança contra esse tipo de incidentes, e como se mantinham informados de tipos de ataques.

O questionário foi aplicado no mês de agosto de 2019, os quais foram respondidos após uma explicação oral sobre o tema e a forma de preenchimento dos questionários, mais precisamente 06 de agosto até 29 de agosto de 2019.

Os dados obtidos na pesquisa foram tabulados através do software Microsoft Excel, onde receberam o tratamento adequado para a apresentação nesta pesquisa. O tratamento das informações e sua análise foram feitas com adaptações de pesquisas sobre “*Ciberseguridad en el Sector Bancario de América Latina y el Caribe*”. O questionário desta pesquisa, foi adaptado do estudo da OEA (2018).

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Neste tópico apresentam-se os resultados obtidos com a aplicação do questionário. Na primeira parte tem-se o perfil dos respondentes e na segunda, as questões específicas sobre *internet banking*.

4.1 PERFIL DOS PARTICIPANTES

Na aplicação da pesquisa, foram obtidos 93 questionários respondidos adequadamente, sendo descartados os incompletos da amostra. Para caracterização do perfil dos discentes, foram elaboradas questões que identifiquem o gênero e a faixa etária. Nesta etapa os resultados obtidos são apresentados nos gráficos 1 e 2:

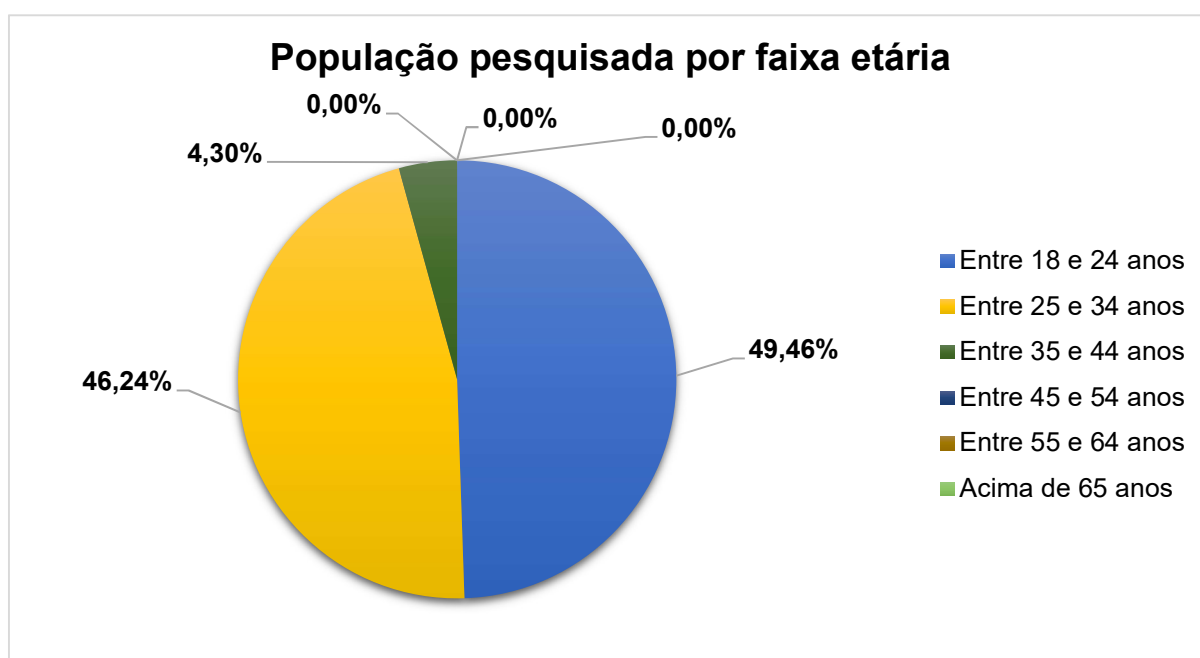


Fonte: Dados da Pesquisa (2019)

De acordo com o gráfico 1, têm-se um equilíbrio entre os graduandos desta instituição. Onde 52,69% é do sexo feminino, com um total de 49 estudantes e 47,31% do sexo masculino, com um total de 44 estudantes. Esses dados acompanham a estatística apontada em pesquisa da FEBRABAN segundo censo de educação superior de 2016.

O gráfico 2 aponta a faixa etária dos graduandos entrevistados na instituição. Os dados evidenciam que se tem uma faixa etária com maior representatividade, esta compreendida entre os 18 a 34 anos, sendo 49,46% dos respondentes entre 18 e 24 anos, o que corresponde a 46 alunos, e com 46,24% dos entrevistados entre 25 e 34 anos, correspondente a 43 respondentes, e apenas 4,30% dos alunos que buscam uma graduação têm entre 35 e 44 anos, estes somando apenas 4 alunos. Já para as demais faixas etárias não houve usuários nesta pesquisa. A “geração Y³” está constantemente conectada e essa realidade condiz com os dados deste gráfico, uma vez que em sua maioria os usuários são os mais jovens.

Gráfico 2 – Faixa etária



Fonte: Dados da Pesquisa (2019)

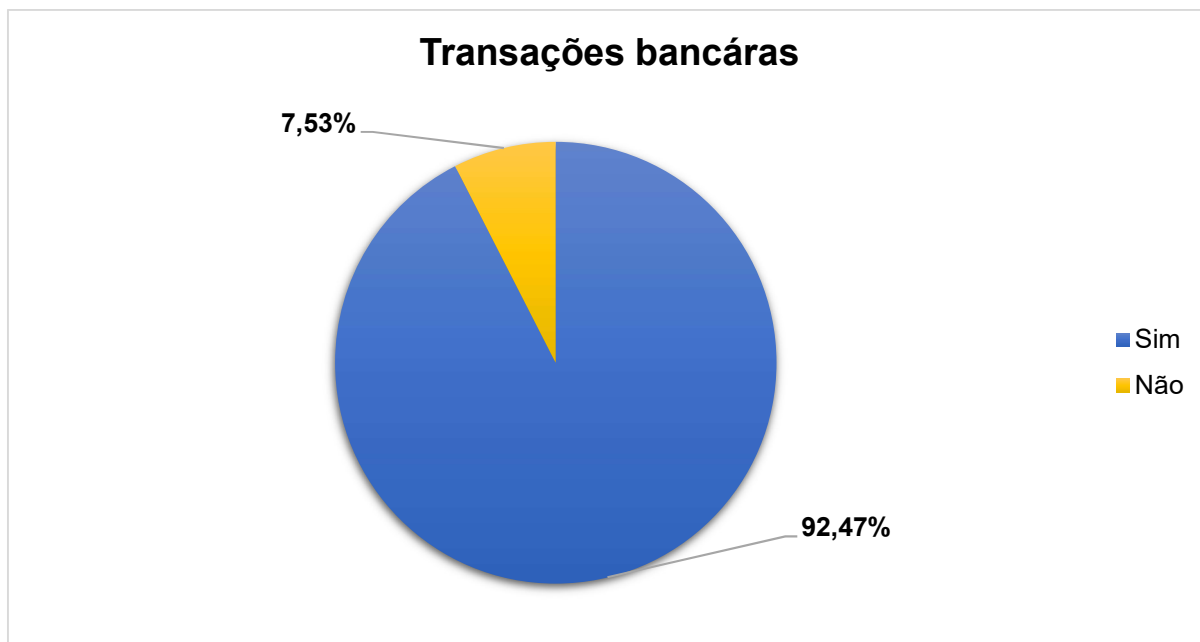
4.2 USUÁRIOS DE OPERAÇÕES BANCÁRIAS POR MEIO DIGITAL

O Gráfico 3 responde as questões a respeito da utilização ou não dos serviços bancários, através dos meios eletrônicos (*smartphones*, *tablets*, computadores, *notebook*, e etc.). A maioria dos entrevistados (92,47%), ou 86 alunos, disse que utiliza os serviços que as instituições financeiras disponibilizam, e 7,53% desses mesmos entrevistados, o que dá apenas 7 alunos, disseram não utilizar desses serviços. A

³ Termo usado para designar as pessoas que nasceram nos últimos anos da década de 1970 até o início da década de 1990.

partir dessa informação é possível afirmar que a tecnologia tem estado presente na vida da maioria dos entrevistados e o uso do *internet banking* tem mudado a forma como as transações bancárias são realizadas atualmente.

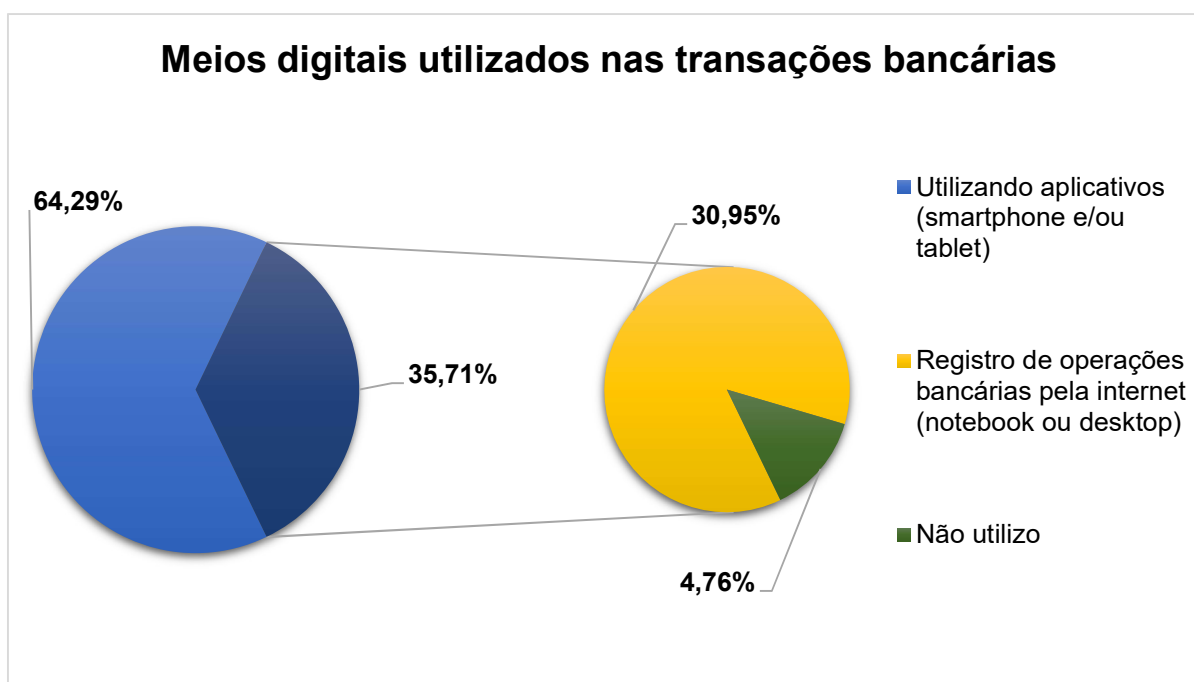
Gráfico 3 – Adeptos das transações bancárias



Fonte: Dados da Pesquisa (2019)

No Gráfico 4, é possível verificar como os entrevistados acessam os serviços bancários, o que demonstra que 64,29% dos graduandos se utilizam apenas de aplicativos nos smartphones e/ou tablets, 35,71% dos alunos se utilizam de aplicativos nos smartphones e/ou tablets, como também, da internet através do navegador de seus computadores e/ou notebooks, sendo que destes, 30,95% dos entrevistados se utilizam apenas de seus computadores e/ou notebooks, e apenas 4,76% não se utilizam de qualquer meio eletrônico para fazer suas operações bancárias. Essa pequena parcela dos entrevistados é alheia à utilização dos meios digitais para realizar transações. No entanto o gráfico mostra que o acesso à tecnologia e a facilidade que ela proporciona tem cada vez mais ganhado espaço.

Gráfico 4 – Meios digitais utilizados nas operações bancárias

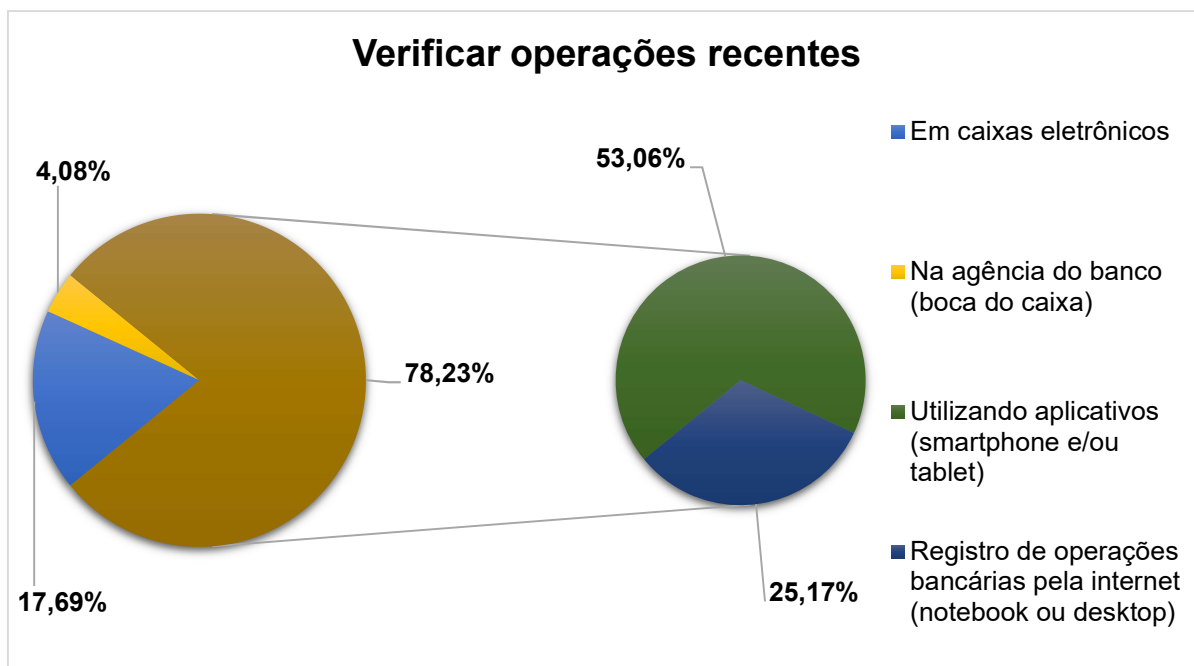


Fonte: Dados da Pesquisa (2019)

No Gráfico 5, temos quais meios os entrevistados verificam as suas transações bancárias, onde 78,23% dos alunos se utilizam de aplicativos nos smartphones e/ou tablets, e da internet através do navegador dos computadores e/ou notebooks, sendo 53,06% deles através de aplicativos nos smartphones e/ou tablets, e apenas 25,17% se utilizam dos computadores e/ou notebooks, e que 17,69% se utilizam dos terminais de caixas eletrônicos, e somente 4,08% dos entrevistados usam os “boca do caixa” de suas agências para fazerem tais operações. Com isso temos que a procura por agências físicas tem diminuído, uma vez que os usuários estão cada vez mais próximos de seus bancos através dos seus dispositivos móveis, tornando isso cada vez mais cômodo ao utilizarem os serviços bancários.

De acordo com o Gráfico 6 tem-se como os entrevistados fazem transferências de recursos, sendo que 72,00% dos respondentes se utilizam de aplicativos nos smartphones e/ou tablets, como também, da internet através do navegador dos computadores e/ou notebooks, sendo 52,00% desses através de aplicativos nos smartphones e/ou tablets, e apenas 20,00% se utilizam dos computadores e/ou notebooks, já para 22,00% dos entrevistados responderam que o fazem através dos caixas eletrônicos, e que apenas 6,00% do total se utilizam da agência do banco para fazerem tais transações.

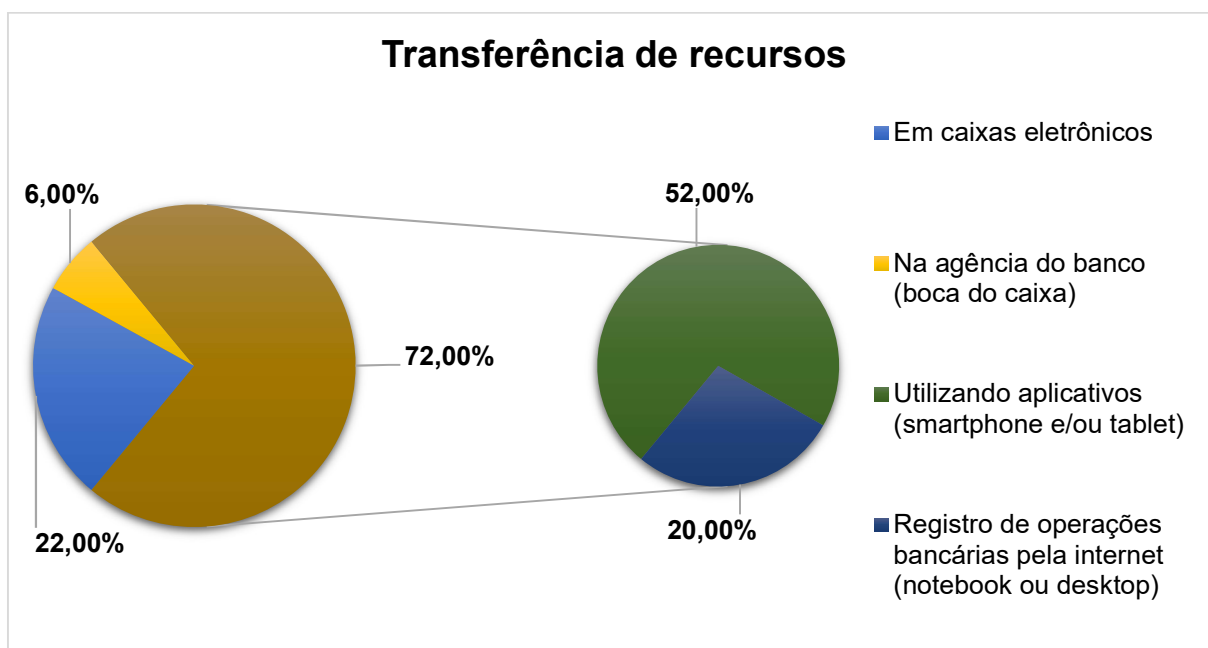
Gráfico 5 – Verificar operações e transações bancárias



Fonte: Dados da Pesquisa (2019)

Os dados do Gráfico 6 se relacionam com os dados do Gráfico 5, uma vez que confirma que a maioria dos usuários respondentes se utilizam de dispositivos móveis para realizar as suas transações, não havendo necessidade de se deslocar até uma agência física do seu banco.

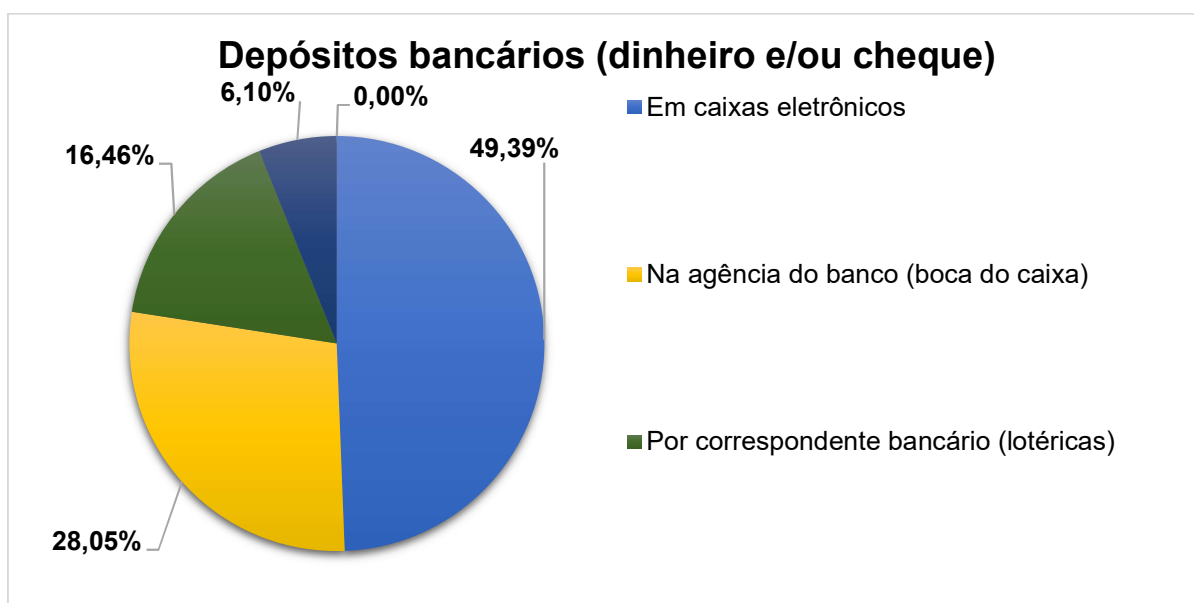
Gráfico 6 – Realização de transferências



Fonte: Dados da Pesquisa (2019)

O Gráfico 7 demonstra como os entrevistados realizam depósitos bancários. De acordo com 49,39% dos entrevistados responderam que utilizam os caixas eletrônicos que as instituições financeiras disponibilizam, e que 28,05% ainda vão as agências fazerem os seus depósitos, 16,46% dos respondentes optam por fazerem nos correspondentes bancários (lotéricas), e que apenas 6,10% do total escolhem fazer através de depósitos eletrônico direto (depósitos esses que são feitos sem envelopes em caixas eletrônicos e que a depender da forma de depósito - dinheiro - a compensação é feito assim que se conclui a transação). A forma mais rápida de realizar um depósito é através de caixa eletrônico sem a necessidade de pessoal para tal operação. Os dados do gráfico confirmam que os entrevistados optam pela rapidez e facilidade na hora de realizar seus depósitos.

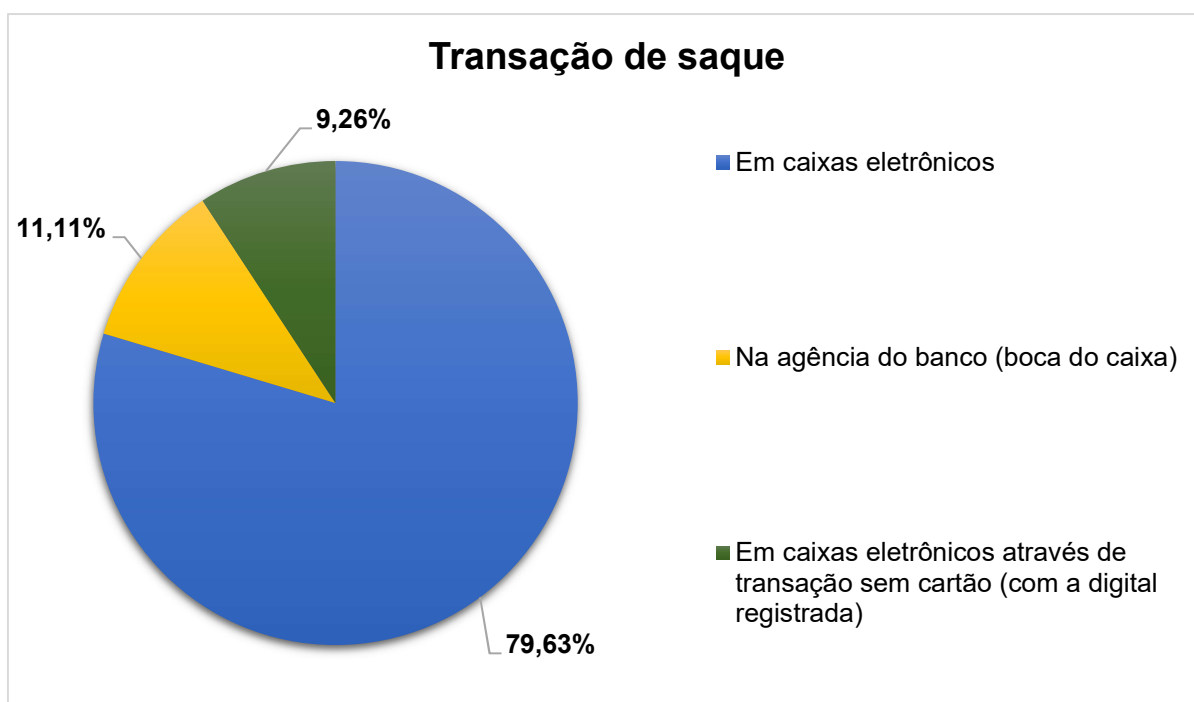
Gráfico 7 – Realização de depósitos bancários



Fonte: Dados da Pesquisa (2019)

No gráfico 8, temos como os respondentes realizam saques de dinheiro de suas agências bancárias. Destes 79,63% dos entrevistados disseram que utilizam dos serviços dos caixas eletrônicos, 11,11% destes alunos responderam que vão até alguma de suas agências bancárias e realizam a retirada de valores em dinheiro na “boca do caixa”, e que 9,26% desses mesmos entrevistados disseram se utilizar dos serviços dos caixas eletrônicos sem a necessidade do cartão da instituição, apenas utilizando-se de sua digital previamente cadastrada.

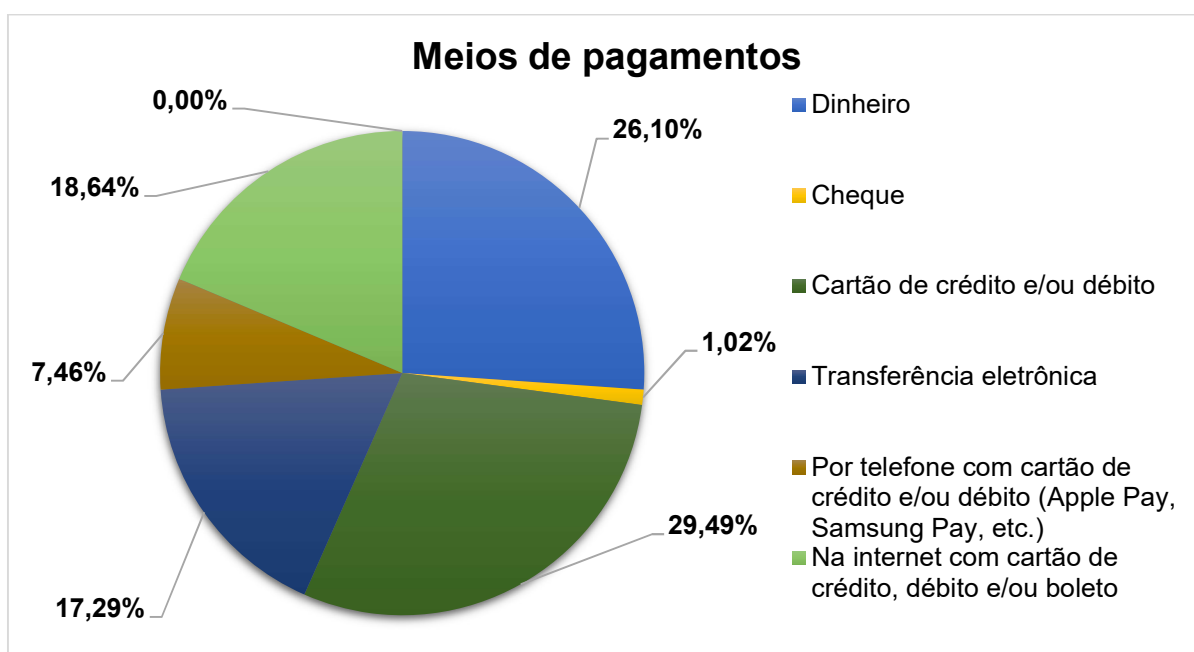
Gráfico 8 – Realização de saques bancários da Pesquisa



Fonte: Dados da Pesquisa (2019)

No gráfico 9, foi perguntado como se davam as suas formas de pagamentos na hora de fazerem compras.

Gráfico 9 – Realização de pagamentos



Fonte: Dados da Pesquisa (2019)

Do qual 29,49% dos entrevistados se utilizam do meio de cartão de crédito e/ou débito, 26,10% dos alunos se utilizam do dinheiro, 18,64% dos consultados na pesquisa usam o cartão de crédito e/ou débito, assim como, do boleto bancário para fazerem os seus pagamentos quando compram na internet, já 17,29% usam da transferência eletrônica para fazerem os seus pagamentos, 7,46% já começam a usar da mais nova ferramenta de pagamento que são dos seus cartões de crédito e/ou débito registrado em seus smartphones, e que apenas 1,02% dos alunos se utilizam da forma de pagamento do cheque.

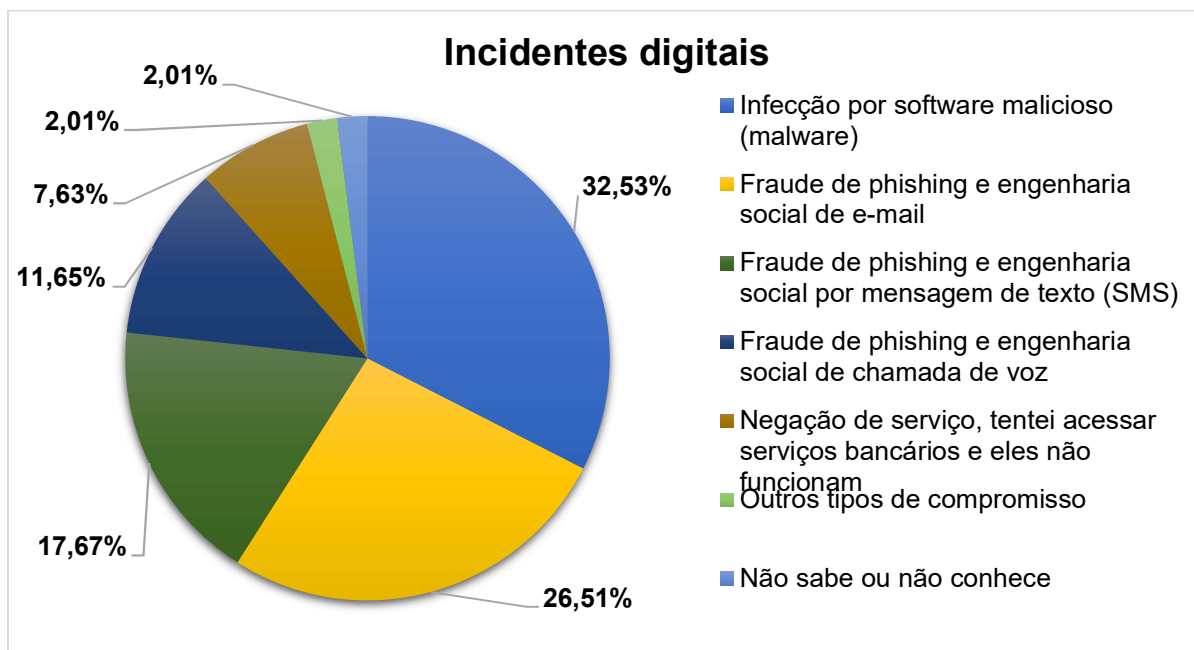
Com as informações do gráfico 9 é possível perceber que para os usuários entrevistados as formas de pagamentos que eles se sentem mais seguros são as de cartões de crédito e/ou débito em todas as suas formas, seja ela física ou virtual, assim como em dinheiro.

4.3 CONHECIMENTO DE CIBERCRIMES

No gráfico 10, tem-se como os entrevistados têm conhecimento sobre alguns dos incidentes digitais, o que demonstra que 32,53% têm conhecimento sobre alguns dos possíveis software maliciosos, o *malware*. Já 26,51% conhecem ou já ouviram falar sobre fraude de *phishing* através de e-mails, e outros 17,67% através de mensagens de texto (SMS), já para 11,65% dos respondentes já passaram por alguma tentativa de fraude através de chamadas de voz, 7,63% dos entrevistados relatam que já passaram por alguma situação da qual tentaram acessar suas informações bancárias e perceberam que algo não estava funcionando normalmente, e 2,01% tiveram outros tipos de compromisso, como também, não souberam ou não conhecem qualquer tipo desses males mencionados.

Esse gráfico 10 demonstra que os entrevistados já passaram ou conhecem os males da vida cibernética em que estão inseridos.

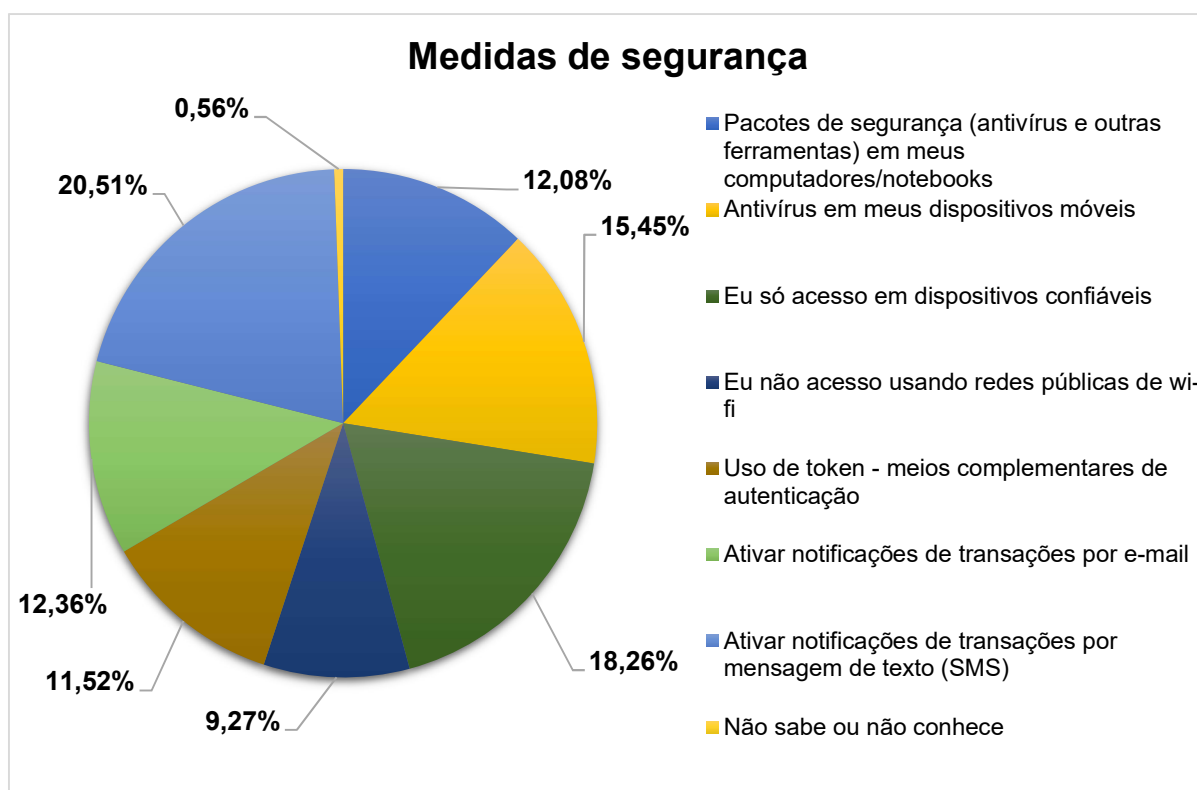
Gráfico 10 – Conhecimentos de incidentes digitais



Fonte: Dados da Pesquisa (2019)

O gráfico 11, demonstra o quão os entrevistados estão cientes dos males e medidas de segurança necessárias para se protegerem, o que se correlaciona com o gráfico anterior, onde 20,51% dos alunos entrevistados se utilizam de pacotes de segurança, 18,26% apenas acessam as suas informações bancárias em dispositivos confiáveis, 15,45% dos alunos respondentes utilizam de antivírus em seus dispositivos móveis, 12,36% dos entrevistados ativam as notificações de suas transações através dos seus e-mails e 12,08% ativam as notificações de suas transações por mensagem de texto (SMS), 11,52% fazem uso do *token* como meio complementar de autenticação de segurança, para 9,27% dos alunos entrevistados responderam que não acessam, aos seus bancos, através de redes de wi-fi públicas desconhecida, e para apenas 0,56% não souberam responder ou não conheciam tais medidas. O que demonstra com as informações do gráfico 11 é que para os usuários entrevistados as medidas de segurança, seja quais elas forem, são preponderantes para poderem acessar as suas informações.

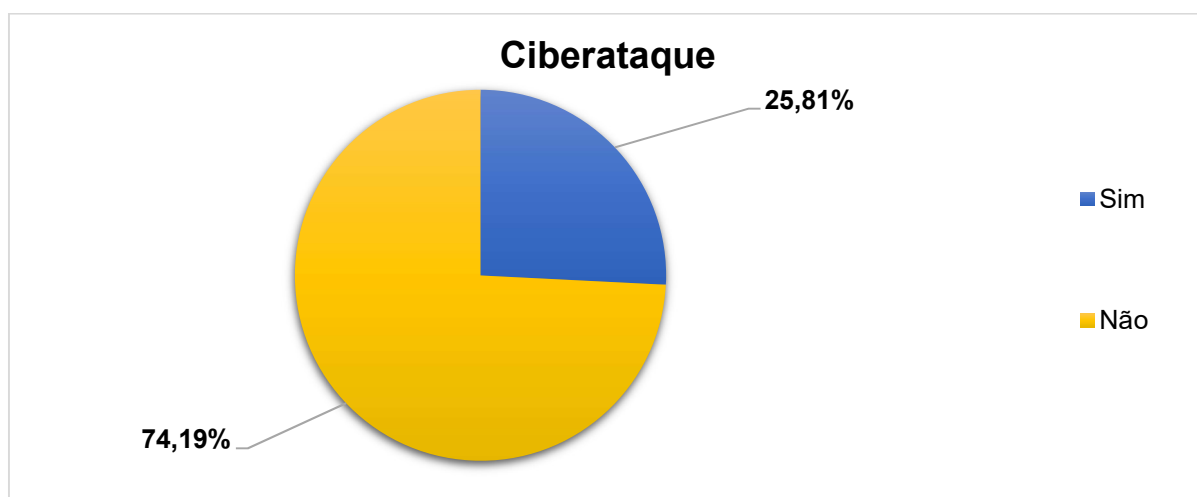
Gráfico 11 – Conhecimentos de medidas contra incidentes digitais



Fonte: Dados da Pesquisa (2019)

O gráfico 12, demonstra que 74,19% dos entrevistados não sofreram qualquer tipo de ciberataque que possa ter comprometido seus dados compartilhados na rede, já para 25,81% já passaram por algum tipo de transtorno por utilizar dos meios digitais. O que evidencia que os entrevistados estão se utilizando das ferramentas necessárias para não sofrerem ataques cibernéticos.

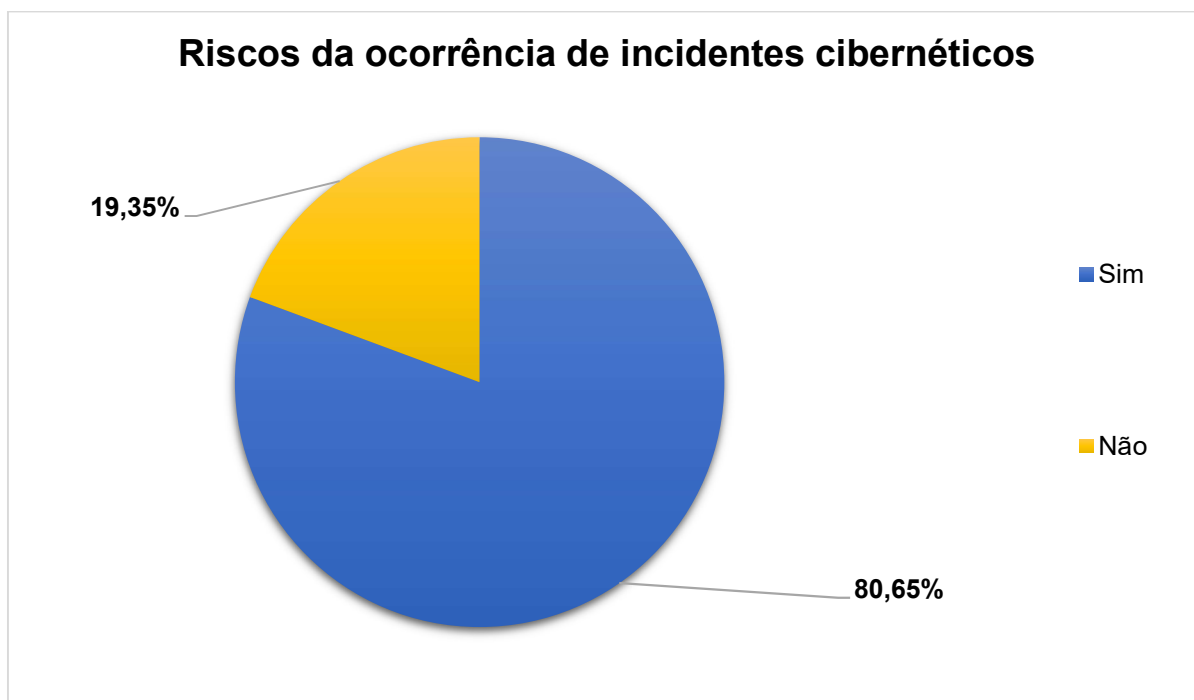
Gráfico 12 – Conhecimentos de ciberataque



Fonte: Dados da Pesquisa (2019)

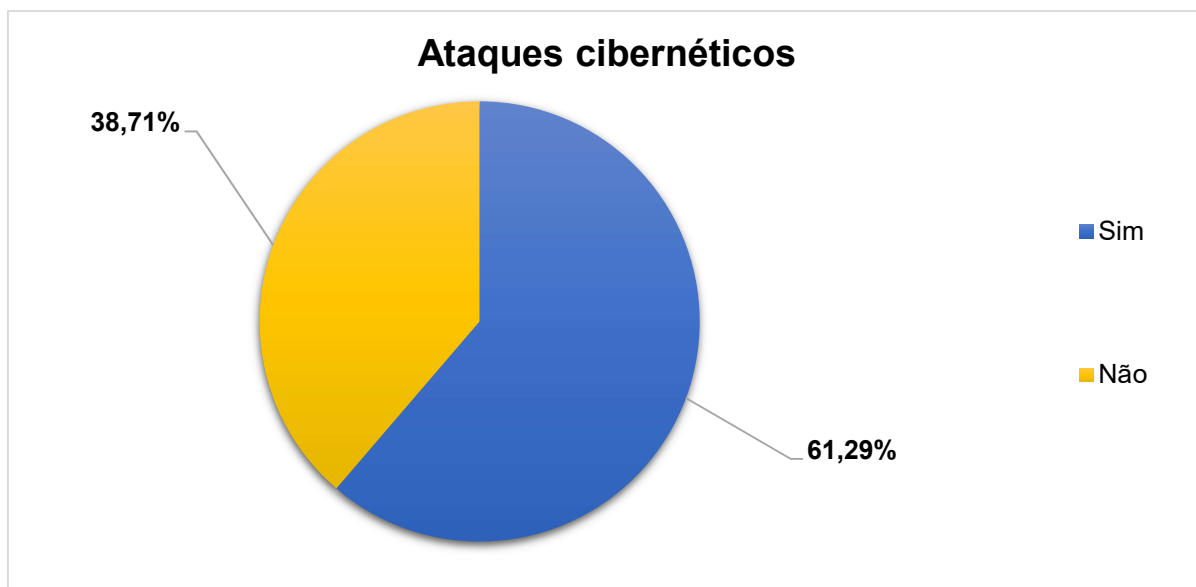
No gráfico 13, lhes fora perguntado do conhecimento dos riscos de incidentes digitais e que apontou que 80,65% do público entrevistado responderam, afirmativamente, que consideram e ponderam na hora da utilização de qualquer meio digital para acessar as suas informações bancárias. Enquanto que para 19,35% não relativizam tais riscos inerentes ao uso dos meios digitais. O que mostra a tendência dos alunos entrevistados de estarem mais prevenidos contra os ciberataques.

Gráfico 13 – Conhecimentos dos riscos de incidentes digitais



Fonte: Dados da Pesquisa (2019)

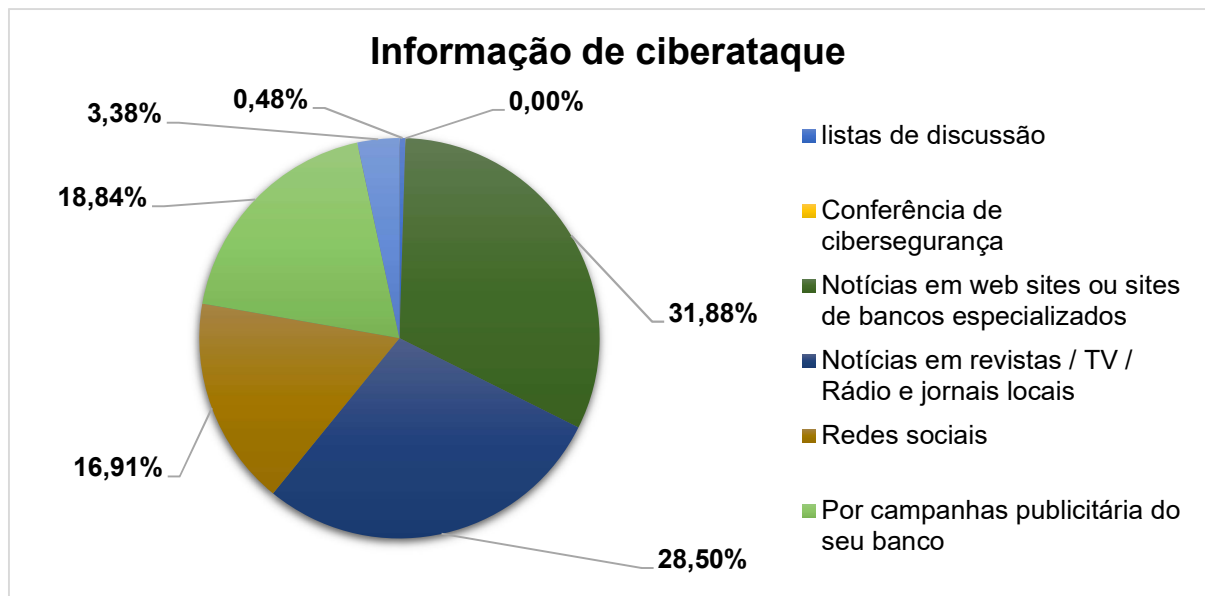
No gráfico 14, vemos que 61,29% dos entrevistados responderam que os ataques às informações bancárias pioraram ou cresceram nos últimos anos. E para 38,71% do público entrevistado não julgaram que tenham piorado. No que diz respeito ao crescimento ou não dos ciberataques os alunos responderam que, em sua maior parte, esses crimes vêm aumentando ano após ano.

Gráfico 14 – Conhecimentos de ciberataque nos últimos anos

Fonte: Dados da Pesquisa (2019)

No gráfico 15, verificou-se que 31,88% dos alunos ficam sabendo das informações sobre cibercrimes através de notícias em websites ou sites de bancos especializados, 28,50% dos entrevistados ficam sabendo através notícias em revistas/TV/rádios e jornais, 18,84% ficam sabendo por meio de campanhas publicitárias do seu banco, 16,91% dos alunos se mantêm informados através das redes sociais, 3,38% não se mantêm informado acerca do assunto, e que apenas 0,48% dos entrevistados entram em alguma lista de discussão a respeito sobre os cibercrimes; não houve respondentes para a conferência de cibersegurança.

Gráfico 15 – Conhecimentos de informações sobre ciber Crimes



Fonte: Dados da Pesquisa (2019)

As informações do gráfico 16 evidenciam que para os alunos entrevistados as informações sobre ciber crimes, seja quaisquer tipos de crime elas forem, influenciam nas suas tomadas de decisões sobre o que e quando acessar tal website e poderem acessar as suas informações.

5 CONSIDERAÇÕES FINAIS

A escolha do tema “cibersegurança” definido a partir do desejo de conhecer e aprofundar este conteúdo, uma vez que antes do desenvolvimento do trabalho o saber era superficial. Durante a pesquisa houve dificuldade para encontrar material teórico da área para elaboração do referencial teórico, quanto à pesquisa de opinião dos entrevistados foram solícitos e não houve problema durante a aplicação.

O trabalho desenvolvido buscou através de pesquisa de opinião constatar a percepção dos usuários de *internet banking* acerca da qualidade e segurança do serviço.

A maioria dos usuários estão na faixa-etária entre 18 e 34 anos conforme foi constatado em pesquisa. Os indivíduos desta faixa fazem parte, ou seja, estão incluídos na era da informação, também conhecida como era digital. Foi concluído que os indivíduos têm buscado formas mais rápidas para solucionar problemas bancários ou mesmo, efetuar transações, seja através de celulares, tablets, computadores ou outros meios digitais, as pessoas optam pela facilidade e velocidade ofertada pelo serviço de *internet banking*, constatando a diminuição da procura por agências físicas.

No tocante à segurança, principal objetivo da pesquisa conclui-se que mais da metade dos usuários entrevistados conhece algum tipo de incidente digital, a exemplo do *malware*, fraude de *phishing* entre outros e, diante disso demonstraram que estão atentos e se utilizam de meios que protegem o usuário contra estas ameaças, utilizando por exemplo pacotes de segurança, antivírus, e etc., e têm consciência que os riscos de acidentes cibernéticos existem e atentam para a sua segurança.

Por fim, conclui-se que os usuários do serviço de *internet banking* estão atentos ao uso correto, aos riscos que oferecem e as formas de proteção disponibilizados pelas agências bancárias têm suprido a necessidade e transmitido confiança através dos seus serviços.

Em contrapartida à pesquisa aplicada com os alunos da instituição, segundo pesquisa nacional do Relatório Global de Fraude e Risco 2019/2020 os indivíduos apontaram que 84% dos brasileiros têm como prioridade de risco o roubo de dados, demonstrando que a confiança dos usuários é diferente do apresentado em amostra do trabalho realizado com os alunos do curso de Ciências Contábeis da UFPB.

REFERÊNCIAS

ANTUNES, Mário; RODRIGUES, Baltazar. **Introdução à cibersegurança: a internet, os aspetos legais e a análise digital forense**. [s. L.]: FCA, 2018.

BINDER DIKER OTTE - BDO. **BDO - retail riskfactor report**. 2017. Disponível em: <https://www.bdo.com/2017-bdo-retail-riskfactor-report>. Acesso em: 08 mar. 2020.

COLLINS, Jill; HUSSEY, Roger. **Pesquisa em administração**. 2. ed. Porto Alegre: Bookman, 2005.

ESTRADA, M. M. P. **A internet banking no Brasil, na América Latina e na Europa**. Revista do Programa de Mestrado em Direito do UniCEUB, Brasília, v. 2, n. 1, p. 138-166, jan./jun. 2005. Disponível em: <http://publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161>. Acesso em: 24 jun. 2019.

FEBRABAN. **Pesquisa FEBRABAN de tecnologia bancária 2019**. 2019. Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf>. Acesso em: 25 jun. 2019.

GIBSON, William. **Neuromancer**. New York: Ace, 1984.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

JUN, M.; CAI, S. The key determinants of internet banking service quality: a content analysis. **International Journal of Bank Marketing**, v.19, n. 7, p. 276- 91, 2001.

KASPERSKY (org.). **O que é cibersegurança?** 2019. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>. Acesso em: 18 jun. 2019.

KROLL'S. Global fraud and risk report 2019/2020 – Mapping the new risk landscape. 2019. Disponível em: <https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2019>. Acesso em: 08 fev. 2020.

MATTAR, A.; TAKAOKA, H. **Critérios de avaliação da qualidade da informação em sistemas de internet banking**. Dissertação (Mestrado em Administração) – Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo. São Paulo: FAE/USP. Disponível em: www.teses.usp.br/teses/disponiveis/12/12139/tde.../alexandremattardf.pdf. Acesso em: 20 jun 2019.

OEA. **Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe**. 2018. Disponível em: <https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf>. Acesso em: 08 fev. 2020.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B. **Metodologia de pesquisa**. 5. ed. Porto Alegre: AMGH, 2013.

SELLTIZ, Claire; WRIGHTSMAN, Lawrence S.; COOK, Stuart W. **Métodos de pesquisa nas relações sociais**. São Paulo: EPU, 1987.

STRONG, D.; LEE, Y.; WANG, R. Data quality in context. **Communications of the ACM**, v. 40, n. 5, p. 104-110, may 1997.

APÊNDICE A – Questionário

**UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS**

QUESTIONÁRIO SOBRE CIBERSEGURANÇA NO SETOR BANCÁRIO

Caro Aluno,

Este instrumento de pesquisa visa auxiliar a elaboração de um Trabalho de Conclusão de Curso (TCC) sobre “Cibersegurança: a percepção dos usuários de *internet banking*”, que está sendo desenvolvido pelo aluno Danyel Targino Pereira, do curso de Ciências Contábeis da UFPB, sob orientação do Prof. Dr. Tiago Henrique de Souza Echternacht, do Departamento de Finanças e Contabilidade da Universidade Federal da Paraíba.

Solicitamos a sua colaboração para responder o presente questionário, como também a sua autorização para apresentar os resultados deste estudo no TCC mencionado. Esclarecemos que a sua participação é voluntária e as respostas serão analisadas conjuntamente, preservando-se o sigilo da fonte.

Caso concorde em participar, por gentileza, responder as questões propostas.

Desde já, agradeço-lhe pela colaboração.

1 - Gênero

- a) (☐) Masculino
- b) (☐) Feminino

2 - Qual a sua faixa etária?

- a) (☐) Entre 18 e 24 anos
- b) (☐) Entre 25 e 34 anos
- c) (☐) Entre 35 e 44 anos
- d) (☐) Entre 45 e 54 anos
- e) (☐) Entre 55 e 64 anos
- f) (☐) Acima de 65 anos

Acerca das operações bancárias, as quais normalmente executa:

3 - Utiliza os meios digitais para suas transações bancárias?

- a) (☐) Sim
- b) (☐) Não

4 - Qual(is) meio(s) digital(is) utiliza para suas transações bancárias?

- a) (☐) Utilizando aplicativos (smartphone e/ou tablet)
- b) (☐) Registro de operações bancárias pela internet (notebook ou desktop)
- c) (☐) Não utilizo

5 - Qual o canal você utiliza para verificar transações recentes e saldos disponíveis?

- a) (☐) Em caixas eletrônicos
- b) (☐) Na agência do banco (boca do caixa)
- c) (☐) Utilizando aplicativos (smartphone e/ou tablet)
- d) (☐) Registro de operações bancárias pela internet (notebook ou desktop)

6 - Como realiza transferência de dinheiro?

- a) (☐) Em caixas eletrônicos
- b) (☐) Na agência do banco (boca do caixa)
- c) (☐) Utilizando aplicativos (smartphone e/ou tablet)
- d) (☐) Registro de operações bancárias pela internet (notebook ou desktop)

7 - De que forma realiza depósitos bancários (cheques e/ou dinheiro)?

- a) (☐) Em caixas eletrônicos
- b) (☐) Na agência do banco (boca do caixa)
- c) (☐) Por correspondente bancário (lotéricas)
- d) (☐) Através de um depósito eletrônico direto (são depósitos feitos sem envelope em caixas eletrônicos e o dinheiro ou cheque depositado é debitado na conta da pessoa favorecida)
- e) (☐) Através de depósito móvel

8 - Qual a forma mais utiliza para realizar saque de dinheiro?

- a) (☐) Em caixas eletrônicos
- b) (☐) Na agência do banco (boca do caixa)
- c) (☐) Em caixas eletrônicos através de transação sem cartão (com a digital registrada)

9 - Quais meios de pagamentos utiliza para fazer compras?

- a) (☐) Dinheiro
- b) (☐) Cheque
- c) (☐) Cartão de crédito e/ou débito
- d) (☐) Transferência eletrônica
- e) (☐) Por telefone com cartão de crédito e/ou débito (Apple Pay, Samsung Pay, etc.)
- f) (☐) Na internet com cartão de crédito, débito e/ou boleto
- g) (☐) Na internet usando moedas virtuais (Ej, Bitcoin, Ethereum, Litecoin, etc.)

10 - Quais os seguintes incidentes digitais que você conhece?

(várias respostas possíveis)

- a) (☐) Infecção por software malicioso (*malware*)
- b) (☐) Fraude de *phishing* e engenharia social de e-mail
- c) (☐) Fraude de *phishing* e engenharia social por mensagem de texto (SMS)
- d) (☐) Fraude de *phishing* e engenharia social de chamada de voz
- e) (☐) Negação de serviço, tentei acessar serviços bancários e eles não funcionam
- f) (☐) Outros tipos de compromisso
- g) (☐) Não sabe ou não conhece

11 - As definições mencionadas anteriormente coincidem com o que você conhecia?

- a) (☐) Não, eu realmente não sabia
- b) (☐) Poucas
- c) (☐) Algumas
- d) (☐) Todas

12 - Quais medidas de segurança você implementou para evitar incidentes digitais?

(várias respostas possíveis)

- a) (☐) Pacotes de segurança (antivírus e outras ferramentas) em meus computadores/notebooks
- b) (☐) Antivírus em meus dispositivos móveis
- c) (☐) Eu só acesso em dispositivos confiáveis
- d) (☐) Eu não acesso usando redes públicas de wi-fi
- e) (☐) Uso de *token* - meios complementares de autenticação

- f) (☐) Ativar notificações de transações por e-mail
- g) (☐) Ativar notificações de transações por mensagem de texto (SMS)
- h) (☐) Não sabe ou não conhece

13 - Conhecia todas as medidas mencionadas anteriormente?

- a) (☐) Não, eu realmente não sabia
- b) (☐) Poucas
- c) (☐) Algumas
- d) (☐) Todas

Antes de continuar, por favor considere a seguinte definição

INCIDENTE CIBERNÉTICO: Situação derivada de um evento intencional ou não intencional que afeta o desenvolvimento de uma atividade no ambiente digital e que gera impacto ou afetação. Para efeitos de futuras perguntas, considere que um incidente é qualificado como tal, desde que a situação tenha tido algum efeito no desenvolvimento das suas atividades como usuário final de um banco.

14 - Você experimentou um incidente ou situação que comprometeu a confidencialidade, integridade ou disponibilidade de suas informações ou seus recursos financeiros em seu banco?

- a) (☐) Sim
- b) (☐) Não

15 - Em geral, você considera que os riscos da ocorrência de incidentes cibernéticos afetam sua decisão de usar mídia digital no setor financeiro?

- a) (☐) Sim
- b) (☐) Não

16 - Em geral, você considera que os riscos da ocorrência de incidentes cibernéticos pioraram no último ano?

- a) (☐) Sim
- b) (☐) Não

17 - Como você se mantém informado sobre novas formas de ataques e ameaças de segurança da informação?

(várias respostas possíveis)

- a) (☐) listas de discussão
- b) (☐) Conferência de cibersegurança
- c) (☐) Notícias em web sites ou sites de bancos especializados
- d) (☐) Notícias em revistas / TV / rádio e jornais locais
- e) (☐) Redes sociais
- f) (☐) Por campanhas publicitária do seu banco
- g) (☐) Não se mantém informado